



POLIZIA DI STATO
CENTRO OPERATIVO SICUREZZA CIBERNETICA
POLIZIA POSTALE E DELLE COMUNICAZIONI
FRIULI VENEZIA GIULIA



UNIVERSITÀ DEGLI STUDI
DI TRIESTE

RINNOVO
PROTOCOLLO D'INTESA
PER LA PREVENZIONE E CONTRASTO
DEI CRIMINI INFORMATICI
SUI SISTEMI INFORMATIVI "CRITICI"
DIPENDENTI DALL'UNIVERSITÀ DEGLI
STUDI DI TRIESTE



POLIZIA DI STATO
CENTRO OPERATIVO SICUREZZA CIBERNETICA
POLIZIA POSTALE E DELLE COMUNICAZIONI
FRIULI VENEZIA GIULIA



UNIVERSITÀ DEGLI STUDI
DI TRIESTE

Il Centro Operativo per la Sicurezza Cibernetica - Polizia Postale per il Friuli Venezia Giulia, con sede in Piazza Vittorio Veneto 1, rappresentato dal Dirigente, dott.ssa Assunta Esposito, in qualità di responsabile del coordinamento e controllo delle attività e servizi della Polizia Postale e delle Comunicazioni, nel proprio ambito territoriale,

e

L'Università degli Studi di Trieste (di seguito denominata "Università di Trieste"), con sede legale in Trieste, Piazzale Europa, 1, C.F. n. 80013890324, rappresentata dal Rettore pro tempore, prof. Roberto Di Lenarda che interviene non in proprio, ma in qualità di rappresentante legale, autorizzato alla stipula del presente atto con delibera del Consiglio di Amministrazione del 23 febbraio 2023 (prot. n. 37924), d'ora innanzi, congiuntamente, le "Parti".

PREMESSO

- che la legge 31 luglio 1997, n. 249, ha istituito l'Autorità per le garanzie nelle comunicazioni dettando norme sui sistemi delle telecomunicazioni e radiotelevisivo;
- che, in relazione all'art. 1, commi 13 e 15 della citata legge, con decreto del Ministro dell'Interno, adottato di concerto con il Ministro delle Comunicazioni e con il Ministro del Tesoro, del Bilancio e della Programmazione Economica, in data 19 gennaio 1999, è stato individuato il Servizio Polizia Postale e delle Comunicazioni del Dipartimento della Pubblica Sicurezza quale organo centrale del Ministero dell'Interno per la sicurezza e la regolarità dei servizi delle telecomunicazioni;
- che l'articolo 39 della legge 16 gennaio 2003, n. 3, recante: "*Disposizioni ordinamentali in materia di pubblica amministrazione*" prevede che il Dipartimento della Pubblica Sicurezza, nell'ambito delle direttive impartite dal Ministro dell'Interno per il potenziamento dell'attività di prevenzione, può stipulare convenzioni con soggetti, pubblici e privati, dirette a fornire, con la contribuzione degli stessi soggetti, servizi specialistici, finalizzati ad incrementare la sicurezza pubblica;



POLIZIA DI STATO
CENTRO OPERATIVO SICUREZZA CIBERNETICA
POLIZIA POSTALE E DELLE COMUNICAZIONI
FRIULI VENEZIA GIULIA



UNIVERSITÀ DEGLI STUDI
DI TRIESTE

- che il decreto legge 27 luglio 2005 n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005 n. 155, recante “*Misure urgenti per il contrasto del terrorismo internazionale*”, ed in Particolare l’art. 7 bis, comma 1, dispone che con decreto del Ministro dell’Interno siano individuate le infrastrutture critiche informatizzate di interesse nazionale, alla cui protezione informatica provvede l’organo del Ministero dell’Interno per la sicurezza e per la regolarità dei servizi di telecomunicazione, operando mediante collegamenti telematici definiti con apposite convenzioni con i responsabili delle strutture interessate;
- che il D.P.C.M. del 17 febbraio 2017, recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale, definisce all’art.1 l’architettura istituzionale deputata alla tutela della sicurezza nazionale relativamente alle infrastrutture critiche materiali e immateriali;
- che il D.P.C.M. del 27 gennaio 2014 ha adottato il “Quadro Strategico Nazionale per la Sicurezza Nazionale dello Spazio Cibernetico e con DPCM 31/03/2017 è stato ridefinito il “Piano Nazionale per la Protezione Cibernetica e la Sicurezza Informatica”;
- che con il D. Lgs. 18 maggio 2018 n. 51, recante “*Attuazione della Direttiva UE 2016/680 del Parlamento Europeo e del Consiglio del 27 aprile 2016*” sono state ridefinite le regole riguardanti il trattamento dei dati personali effettuato per “finalità di polizia”, ovvero direttamente collegate all’attività di prevenzione e repressione dei reati e di tutela dell’ordine e della sicurezza pubblica;
- che con il Decreto 19 settembre 2017, n. 215 del Ministero dell’Interno, di concerto con i Ministri dello Sviluppo Economico e dell’Economia e delle Finanze, è stato adottato il “*Regolamento recante individuazione delle denominazioni, degli stemmi, degli emblemi e degli altri segni distintivi in uso esclusivo alla Polizia di Stato e al Corpo nazionale dei vigili del fuoco, nonché le modalità attuative ai fini della loro concessione in uso temporaneo a terzi*”;
- che la Direttiva del Ministro dell’Interno del 15 agosto 2017 “sui comparti delle Specialità e sulla razionalizzazione dei Presidi di Polizia” ha ribadito al punto 1.4 la competenza della Polizia Postale e delle Comunicazioni in materia di protezione delle infrastrutture critiche nonché di sicurezza e regolarità dei servizi di telecomunicazione;



POLIZIA DI STATO
CENTRO OPERATIVO SICUREZZA CIBERNETICA
POLIZIA POSTALE E DELLE COMUNICAZIONI
FRIULI VENEZIA GIULIA



UNIVERSITÀ DEGLI STUDI
DI TRIESTE

- che nell'ambito della direttiva generale per l'attività amministrativa e per la gestione relativa all'anno 2023, il Ministro dell'Interno, in ordine agli obiettivi operativi, nel ribadire l'esigenza di tutelare dalle minacce cyber coloro che operano nel mondo della rete, anche attraverso appositi contatti bilaterali (intese, riunioni, accordi, ecc.) tra l'amministrazione e gli enti gestori di sistemi e servizi strategici, ha altresì previsto il rafforzamento – attraverso le risorse del PNRR – delle difese cibernetiche, aumentando il grado di resilienza informatica dell'amministrazione attraverso la creazione di sezioni operative per la sicurezza cibernetica distrettuali, di laboratori operativi dotati delle infrastrutture per le attività forensi (CLABS) e il potenziamento della sala server, al fine di prevedere o rilevare tempestivamente attacchi e incidenti informatici;
- che, con decreto del Capo della Polizia del 28 giugno 2022, è stata attuata la complessiva revisione dell'assetto ordinativo delle articolazioni periferiche dell'Amministrazione della Pubblica Sicurezza e, in particolare, dei Centri Operativi per la Sicurezza Cibernetica (C.O.S.C.) quale nuova denominazione dei Compartimenti di Polizia Postale e delle Comunicazioni, al cui interno sono stati istituiti i Nuclei Operativi Sicurezza Cibernetica (N.O.S.C.);
- che con il D. Lgs. 18 maggio 2018 n. 65 è stata recepita la Direttiva (UE) 2016/1148 del Parlamento Europeo e del Consiglio del 6 luglio 2016, recante “*misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione*” (c.d. Direttiva NIS), che individua quale Autorità di contrasto il Servizio Polizia Postale e delle Comunicazioni in qualità di organo centrale del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione, di cui all'articolo 7-bis del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n.155, così come individuato dal Decreto Interministeriale del 10 gennaio 1999;
- che il Centro Operativo per la Sicurezza Cibernetica - Polizia Postale per Friuli Venezia Giulia provvede, come organo periferico del Servizio Polizia Postale e delle Comunicazioni del Dipartimento della Pubblica Sicurezza, ad assicurare i Servizi della Polizia Postale e delle Comunicazioni, con particolare riferimento alla prevenzione e repressione dei reati commessi avvalendosi delle specifiche potenzialità tecniche dei servizi o mezzi di comunicazione, anche ad alta tecnologia, ovvero alterando il normale funzionamento degli stessi;



POLIZIA DI STATO
CENTRO OPERATIVO SICUREZZA CIBERNETICA
POLIZIA POSTALE E DELLE COMUNICAZIONI
FRIULI VENEZIA GIULIA



UNIVERSITÀ DEGLI STUDI
DI TRIESTE

- che le reti telematiche di supporto alle funzioni istituzionali dell'Università degli Studi di Trieste sono da considerare infrastrutture sensibili di interesse pubblico. Risulta, pertanto, necessario prevenire e contrastare ogni forma di accesso illecito, anche tentato, con finalità di:
 - a) interruzione dei servizi di pubblica utilità;
 - b) indebita sottrazione di informazioni;
 - c) porre in essere qualsiasi ulteriore attività illecita;
- che in data 29 gennaio 2021, le Parti hanno sottoscritto un Protocollo d'Intesa di durata triennale per la prevenzione ed il contrasto dei crimini informatici sui sistemi informativi dell'Università degli Studi di Trieste, elaborando un modello operativo di collaborazione per la prevenzione ed il contrasto dei crimini informatici che hanno per oggetto, nella loro complessità, i sistemi ed i servizi informatici "critici" dell'Ente;
- che le Parti, in forza della proficua collaborazione sin qui svolta, ritengono opportuno procedere al Rinnovo dell'accordo in vigore;
- per l'attuazione e la gestione delle attività di cui al successivo art. 1, le Parti designano ciascuna un referente con il compito di definire congiuntamente le linee di azione comuni verificandone periodicamente la realizzazione. Per l'Università di Trieste il referente è tenuto a presentare all'Ateneo una relazione annuale sull'attuazione della Convenzione, e viene individuato nel dott. Giorgio Giorgetti; per il Centro Operativo il referente viene individuato nel Direttore Tecnico Capo Dott. Giuseppe Panarello. In caso di sostituzione del proprio referente ciascuna Parte informerà l'altra entro trenta giorni con comunicazione scritta.
- che la cooperazione tra il Centro Operativo per la Sicurezza Cibernetica - Polizia Postale per il Friuli Venezia Giulia e l'Università degli Studi di Trieste, volta alla prevenzione e alla repressione dei crimini informatici, ispirata al principio di sicurezza partecipata, nell'intento di assicurare in via sinergica ed efficiente le risorse del Sistema Paese a vantaggio dell'intera collettività, contribuisce al contenimento dei costi operativi derivanti da interruzioni dei servizi erogati attraverso sistemi informatici e di telecomunicazioni.



POLIZIA DI STATO
CENTRO OPERATIVO SICUREZZA CIBERNETICA
POLIZIA POSTALE E DELLE COMUNICAZIONI
FRIULI VENEZIA GIULIA



UNIVERSITÀ DEGLI STUDI
DI TRIESTE

TUTTO CIO' PREMESSO
LE PARTI STIPULANO E CONVENGONO QUANTO SEGUE

Articolo 1

1. Le Parti si impegnano a rinnovare un piano di collaborazione volto:
 - a) alla condivisione e all'analisi di informazioni idonee a prevenire e contrastare attacchi o danneggiamenti in pregiudizio delle infrastrutture informatiche dell'Università degli Studi di Trieste per le finalità meglio in premessa specificate;
 - b) alla segnalazione di emergenze relative a vulnerabilità, minacce ed incidenti in danno della regolarità dei servizi di telecomunicazione;
 - c) all'identificazione dell'origine degli attacchi che abbiano come destinazione le infrastrutture tecnologiche gestite dall'Università degli Studi di Trieste o che traggano origine dalle medesime;
 - d) alla realizzazione e alla gestione di attività di comunicazione fra le Parti per fronteggiare situazioni di emergenza.

2. Le attività necessarie al conseguimento degli obiettivi di cui al precedente comma 1 verranno assicurate dal Centro Operativo per la Sicurezza Cibernetica - Polizia Postale per il Friuli Venezia Giulia e dall'Università di Trieste.

Articolo 2

1. Le Parti potranno sviluppare attività formativa congiunta sui sistemi e sulle tecnologie informatiche utilizzate, nonché sulle procedure di intervento atte a prevenire e contrastare gli accessi illeciti o i tentativi di accesso illecito ai danni di tali sistemi e tecnologie nonché i fenomeni delittuosi di cui all'art. 1.



POLIZIA DI STATO
CENTRO OPERATIVO SICUREZZA CIBERNETICA
POLIZIA POSTALE E DELLE COMUNICAZIONI
FRIULI VENEZIA GIULIA



UNIVERSITÀ DEGLI STUDI
DI TRIESTE

2. Le parti convengono che il proprio personale possa fruire a titolo gratuito delle attività didattiche erogate sotto forma di corsi di formazione o, per il personale della Polizia Postale, di corsi singoli all'interno dei corsi di laurea attivati dall'Università degli Studi di Trieste, anche in deroga ai termini di iscrizione ordinariamente previsti. La partecipazione a tali attività potrà avvenire sia tramite semplice frequenza che con il sostenimento delle eventuali prove finali o di profitto.

Articolo 3

1. Le Parti cooperano al fine di realizzare eventuali tecnologie necessarie per rendere operativo il presente Protocollo d'Intesa, il cui oggetto primario è rappresentato dalla collaborazione da parte della Polizia Postale e delle Comunicazioni, anche attraverso l'interscambio di dati, finalizzata ad incrementare i livelli di prevenzione e contrasto dei crimini informatici ai danni dei sistemi gestiti dall'Università degli Studi di Trieste, gli accordi di collaborazione, in coerenza con l'art. 39, comma 2, della L. 16 gennaio 2003, n. 3 e saranno oggetto di successivi atti aggiuntivi al presente Protocollo d'intesa, e comunque sottoposti all'approvazione dei competenti organi accademici.
2. Nessun onere economico specifico deriva dal presente accordo per l'Amministrazione della Pubblica Sicurezza e per l'Università degli Studi di Trieste.

Articolo 4

1. Le parti si impegnano a sviluppare iniziative congiunte, concordate preventivamente, volte a valorizzare il reciproco rapporto di collaborazione, anche tramite l'utilizzo delle denominazioni, degli stemmi, degli emblemi e degli altri segni distintivi in uso esclusivo alla Polizia di Stato, nel rispetto del decreto del Ministro dell'Interno 19 settembre 2017, n. 215.
2. Con riferimento al precedente comma 1, l'Università degli Studi di Trieste si impegna a promuovere i rispettivi brand, anche attraverso la realizzazione di spot dedicati da trasmettere sulle principali piattaforme social ovvero a mezzo stampa sui principali quotidiani, sempre con il coordinamento del competente



POLIZIA DI STATO
CENTRO OPERATIVO SICUREZZA CIBERNETICA
POLIZIA POSTALE E DELLE COMUNICAZIONI
FRIULI VENEZIA GIULIA



UNIVERSITÀ DEGLI STUDI
DI TRIESTE

Ufficio relazioni esterne, cerimoniale e studi storici della Segreteria del Dipartimento.

Articolo 5

1. Le Parti si impegnano a trattare ed a custodire i dati e le informazioni personali acquisite nell'ambito delle attività previste dal presente Protocollo d'Intesa nel rispetto della normativa in materia di protezione dei dati personali.
2. Ciascuna Parte si impegna a mantenere riservati ed a non utilizzare i risultati delle attività svolte in comune senza il preventivo consenso scritto dell'altra Parte.
3. L'obbligo di riservatezza di cui al comma che precede permarrà anche successivamente all'estinzione del presente Protocollo d'Intesa.
4. Le Parti si impegnano a far osservare ai propri ausiliari, dipendenti, e/o collaboratori le norme, le regole, le procedure ed i principi, per quanto applicabili, contenuti nei rispettivi codici etici e codici di comportamento.

Articolo 6

3. Il presente Protocollo, che entra in vigore dalla data della sottoscrizione, ha durata di tre anni e può essere ulteriormente rinnovato con accordo scritto tra le parti;

Articolo 7

1. Ogni controversia relativa all'interpretazione ed all'esecuzione del presente Protocollo d'Intesa viene esaminata bonariamente dalle Parti.
2. Le Parti potranno recedere dal presente accordo senza onere alcuno, previo preavviso scritto non inferiore a trenta giorni.
3. A tutti gli effetti di legge, l'Università di Trieste dichiara di eleggere domicilio in Trieste, Piazzale Europa 1, PEC: ateneo@pec.units.it; il C.O.S.C. dichiara di



POLIZIA DI STATO
CENTRO OPERATIVO SICUREZZA CIBERNETICA
POLIZIA POSTALE E DELLE COMUNICAZIONI
FRIULI VENEZIA GIULIA



UNIVERSITÀ DEGLI STUDI
DI TRIESTE

eleggere domicilio in Trieste, Piazza Vittorio Veneto 1, PEC:
dipps504.0000@pecps.poliziadistato.it.

Letto, approvato e sottoscritto.

Luoghi e date delle firme digitali

IL DIRIGENTE
DEL C.O.S.C. POLIZIA POSTALE
FRIULI VENEZIA GIULIA
Vice Questore della P. di S.
Dott.ssa Assunta ESPOSITO

IL MAGNIFICO RETTORE
DELL'UNIVERSITÀ DEGLI STUDI
DI TRIESTE

Prof. Roberto DI LENARDA

VISTO
IL QUESTORE DELLA PROVINCIA DI TRIESTE
Dott. Pietro OSTUNI
